Click here to view PowerPoint presentation; Press Esc to exit

The Challenges of Internetworking Unattended Autonomous Sensors

Alessandro Berni, Diego Merani, Michel Leonard
NATO Undersea Research Centre
Viale S. Bartolomeo, 400
19138 La Spezia
ITALY

Netcentric@nurc.nato.int

ABSTRACT

New paradigms for Network Enabled Capabilities and Network Enabled Warfare, which are being developed by NATO and its member nations, will see the emergence of a new generation of autonomous sensors designed to operate without human supervision, and capable of enhancing system effectiveness by collaborating with neighbouring nodes.

Several trade-offs exist between the different components of such resource-limited sensors (e.g. power consumption, processing power, network communications) that have to be taken into account to reach a workable solution that meets the requirements. The design of such innovative sensors will therefore require a holistic approach, to realize a balanced compromise between sensor capabilities and their integration with network infrastructures.

This paper starts by defining the physical peculiarities that characterize unattended autonomous sensors and then discusses issues specific to classified sensors, such as protection from physical compromise against loss of information or tampering.

The challenges deriving from internetworking such sensors on a local area or across a wide area network will then be discussed, from a perspective that mirrors the ISO/OSI network model. The issues of information protection (INFOSEC) will then be analysed, to touch some of the available methodologies to ensure integrity, authentication and confidentiality, together with the accompanying key distribution and management services. While the principal focus of this work is on maritime networks, the considerations presented can be similarly applied to other types of sensors.

1.0 INTRODUCTION

Sensor networks will play an important role in NATO's Network Enabled Capability (NNEC). The scope and size of those networks will vary on the basis of the sensing capabilities to be provided (e.g. acoustic, seismic, magnetic, infrared, radar, and video) and the security implications for activities such as expeditionary operations support, port protection or undersea surveillance, will be more vital that those found in many civilian applications.

In this paper, we start by defining the physical peculiarities that characterize unattended autonomous sensors (such as acquisition and processing capabilities; considerations on the amount of on-board processing and data reduction that is advisable; available power sources; limiting factors such as maximum antenna height and total technical volume). Specific issues of classified sensors will also be discussed, such as protection from physical compromise against loss of information or tampering.

Berni, A.; Merani, D.; Leonard, M. (2006) The Challenges of Internetworking Unattended Autonomous Sensors. In *Military Communications* (pp. 2-1 – 2-14). Meeting Proceedings RTO-MP-IST-054, Paper 2. Neuilly-sur-Seine, France: RTO.
Available from: http://www.rto.nato.int/abstracts.asp.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
DEC 2006	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The Challenges of Internetworking Unattended Autonomous Sensors	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **NATO Undersea Research Centre Viale S. Bartolomeo, 400 19138 La Spezia ITALY**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM202750. Military Communications (Les communications militaires), The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**35**	

We will then discuss the challenges deriving from internetworking such sensors on a local area or across a wide area network, taking a perspective that mirrors the ISO/OSI network model. The issues of information protection (INFOSEC) will then be analysed, to touch some of the available methodologies to ensure integrity, authentication and confidentiality, together with the accompanying key distribution and management services.

1.1 Sensor Networks: Scope and Purpose

The primary purpose of sensor networks is to detect and report events occurring within detection range: basic functions of a sensor node include event detection, event or target classification, target tracking, and event reporting. Sensor networks offer a cost-effective approach to detect low-signature targets (reducing errors and improving tracking and targeting) and to support the Operational Picture.

This improvement of the sensing function is possible through the cooperation between different nodes of the network: the wireless component plays therefore a key role not only to report events to a remote command, but also to support the cooperation between the sensor nodes.

This operation of sensor networks normally occurs in a physically demanding environment. The nature of the deployments exposes the sensors to detection and compromise: the risks of denial of service, node displacement or removal, false data injection, have to be countered using limited resources on battery-powered platforms. To make things more challenging, the communications environment may be difficult, due to fading and sub-optimal antenna positioning, coupled with low population density of sensor nodes. The more the spacing between the nodes is increased (up to several nautical miles between one node and the other), the higher the probability of intercept. In the case of drifting sensors in maritime surveillance networks the changing network topology may introduce an additional level of complexity. Nodes may also be added at any time to replace nodes that have lost power or that have been destroyed.

From the software point of view sensors normally employ embedded operating systems to provide real-time performance. The specific sensing application is normally customized, and is sitting on a commercial-off-the-shelf (COTS) operating system. The general assumption that we are making is that the operating system is not necessarily trusted but at least it has to be considered dependable, not bypassable, and capable of implementing correctly the documented interfaces, disallowing unintended execution or access.

But probably the greatest limiting factor to the sensor's capability and life expectancy lies in the capacity of the batteries. This capacity is limited and design must account this fact, incorporating techniques for energy conservation both at the node level and at the network level: as an example different choices in the routing strategy can impact the energy levels not only on the transmitter, but also on the receiver nodes.

The behaviour of nodes can vary on the basis of the mission assigned: as an example, upon the detection of an event of interest, the sensor may relay the information directly to the Command or may start collaborating with other nodes to reduce its probability of false detection, or to perform target tracking.

Basic mission types involve the defence of a perimeter or the denial of an area (e.g. for port protection), and covert remote surveillance (e.g. in preparation of amphibious operations).

In perimeter defence missions, aimed at the detection and tracking of targets that cross a specified border, the sensor positioning is usually one-dimensional (e.g. along linear barriers) leading to a topology that is mostly static, with few node additions or deletions in the course of time.

As an example, the nodes of maritime surveillance networks can be drifting, moored to the bottom at chosen depths or laid directly on the seabed. The moderate gain receivers, which may be used also in

passive mode, have the advantage of no own ship noise and can be laid to form a large network extended over wide areas. The covertness of receivers suits operations in critical areas and improves chances of detection of unaware submarines (that optimise their course only with respect to the transmitter position) with either a favourable aspect angle or Doppler shift. Elementary detection volumes can be overlapped: each node has an independent opportunity to detect the target, and inter-sensor data fusion can be used to reduce false alarms and exploits deployment geometry to enhance localization and tracking.

Such systems, while normally deployed in the vicinity of friendly forces, can also be applied to remote surveillance missions, which are typically conducted in areas of crisis or behind enemy lines, where the sensors will be unattended for long periods of time, and operation will be possible only until the batteries run out of capacity. This implies that in all cases the system has to be capable of working unattended and in autonomy.

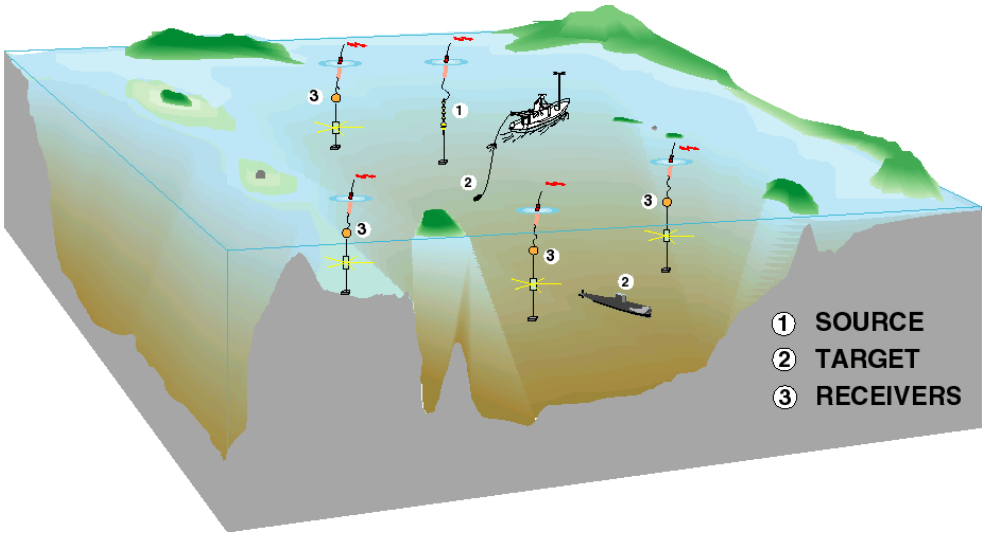


Figure 1: example of a maritime surveillance network

1.2 Communications Architecture

Sensor networks have many characteristics in common with ad-hoc networks, as well as complementary requirements to ensure additional flexibility: for example, the membership and role of a sensor in a network may not be known before the network is actually deployed. Nodes may disappear from the network either temporarily (during sleep cycles) or permanently: the network must have the capability of self-reorganization, using a routing technique that is suitable to support complex topologies and has fast convergence. Network re-organization as nodes are added or removed is an ongoing process, which ensures a proper energy balance across the network. The result is a resilient organization, where loss of a fraction of the nodes leads to a graceful decrease of network performance.

This architecture can be modelled using a perspective that mirrors the ISO/OSI layered stack: the physical layer provides the wireless link between connected nodes, and the network layer ensures support to routing and data delivery across the network, probably using a reliable transport mechanism. In addition to that, several applications will be supported at the application layer. Using the ISO/OSI reference model allows the customisation of those layers that are most critical to satisfy the ad-hoc networking requirements. As an example a specific deployment project may choose to retain the higher levels, such as TCP and above, but choosing a different data link layer, which is more suited, for example, to connect a smaller number of nodes.

1.2.1 Layer 1 and 2: physical and data link

The physical and data link layers are the lowest in the ISO/OSI network model. When discussing the physical layer in the context of sensor networks, we normally assume that communications occur using a wireless medium (normally radio frequency, although alternative media such as underwater acoustic communications are now becoming of interest).

The use of spread spectrum for the wireless communication, in association with burst transmission patterns, can be used to optimise battery life and to reduce the probability of detection by electronic means.

As noted by Carlson in his textbook [1], a particular concern is the question of the fractional bandwidth, defined as absolute bandwidth divided by centre frequency. Hardware costs and complexity are minimized if the fractional bandwidth is kept within 1-10%. The consequence is that signals with a large bandwidth should be modulated on high-frequency carriers. The information rate is proportional to bandwidth, according to the Hartley-Shannon law: a high information rate requires therefore a high carrier frequency.

In a civilian context, many popular COTS solutions for wireless communications can be applied, which normally operate in the Industrial, Scientific and Medical (ISM) unlicensed frequency bands. The availability of low cost integrated devices enables the creation of very small sensors at a very low cost.

The adherence to recognized standards together with appropriate choices in the frequency bands, providing sufficient bandwidth and unlicensed operations, allows the installation of sensor networks anywhere in the world. The alternative would be to individually request a license for every sensor node or network to be deployed: a clearly unpractical approach for many civilian applications targeted at the mass market.

Reliance on unlicensed frequency bands, while being very practical for civilian applications, may not be as well appropriate in a military context. As an example, the ISM band does not guarantee protection from interference and very powerful low-cost 2.4 GHz jammers can be built using simple devices such as microwawe ovens. This suggests that mission critical sensor networks supporting the NNEC should communicate using military frequencies with the required level of protection. The Frequency Management Sub-Committee (FMSC) of the NATO C3 Board is specifically addressing the implications of the introduction of new wideband digital communications systems (e.g. software radios and next-generation sensor networks) into the military frequency spectrum.

1.2.1.1 MAC Protocols

Media Access Control (MAC) protocols for multihop wireless networks have been extensively studied and a considerable amount of work has been conducted in this field in the past 30 years. They can be divided in two categories, contention-based and schedule-based. One of the most widespread contention-based mechanisms, Carrier Sense Multiple Access (CSMA), forms the basis for widespread standards such as 802.11, together with its variations required to satisfy requirements such as higher data rates, enhanced MAC security or quality of service.

Control of the transmit power levels for wireless networks is a definite requirement, to adjust the RF emission to the desired communications range: typically this level will be optimized as a function of the physical spacing between the nodes, but nodes taking the role of gateway for a network will have the additional capabilities and power to support longer range transmissions back to a command centre.

From the energy consumption perspective, an additional issue exists with contention-based MAC mechanisms, where the nodes consume energy also when they are not transmitting or receiving. This has been tackled only lately, with proposals for new MAC protocols.

Recent papers present solutions for saving energy that are based on meticulous power-off strategies. Those apply well to networks of simple sensors, which present a comparable power balance during the transmit, receive or idle states, and the power-off of the radio component is a viable way to save energy. In more complex sensor systems this saving may simply go unnoticed, since the transducers and the on-board processors may have a power balance that is larger by orders or magnitude.

To give an example, S-MAC, by Ye et al. [2], is inspired by the IEEE 802.11 MAC and developed along three techniques: a) the sleep periods of neighbouring nodes are auto-synchronized, b) the radio is set to sleep state also during the transmissions of other nodes, c) message passing is used to reduce contention latency for sensor-network applications that require store-and forward processing as data move through the network. The results on a sample sensor node (the “Mote” developed at the UC Berkeley) show that, on a source node, an 802.11-like MAC consumes 2–6 times more energy than S-MAC for traffic load with messages sent every 1–10s.

Van Dam et al have proposed [3] a variation of S-MAC based on the dynamic termination of the radio duty cycle. Under homogeneous load the results are comparable to those of S-MAC, but in a scenario of variable load a factor of 5 improvement has been observed.

The TRAMA traffic-adaptive medium access protocol, proposed by Rajendran et al. [4], differs from the contention-based S-MAC a) for being schedule-based and therefore inherently collision-fee b) for using a dynamic approach based on current traffic to switch nodes to low-power mode.

As a general rule, schedule-based MACs present higher delays that those based on contention: TRAMA and other schedule-based mechanisms that may be developed in the future are therefore better suited to energy-efficient applications that require high delivery assurance (e.g. data collection and monitoring applications).

1.2.2 Layers 3 and 4: network and transport

At the network layer, limited energy resources are again a factor to be taken in careful consideration since the early stages of the design of the system. Should some nodes become focal point of the communications across the network, those will inevitably spend more energy than less active ones. Periodic re-routing would then be required to balance the energy consumption across the network.

Automatic network self-organization is an important requirement, both at the time of the initial deployment, as well as in a later stage, to allow for the addition and deletion of nodes. Nodes may be added to expand the coverage area of a network. Nodes may disappear from the network because they run out of battery or following physical destruction. In either case continuity in communications (and in trust) has to be properly supported.

Routing decisions in multi-hop networks are made according to routing tables that are built on link cost, accounting the energy required to transmit and receive. In order to transparently allow this flow, it is required that the packer header field is not encrypted.

To build its routing table every node has to detect its neighbour nodes: the decision on the actual routing strategy and its efficiency in terms of energy will depend on the routing algorithm.

The study of routing protocols is a very active area, and the major focus so far has been on mobile networks, where the need for frequent path updates conflicts with low duty cycles to extend battery life. The best example is the work of the MANET working group of the IETF, whose goal is to write a standard for Internet-based mobile ad hoc networking. Protocols in this category include the temporally ordered routing algorithm (TORA), the ad hoc on demand distance vector protocol (AODV), the

destination-sequenced distance vector protocol (DSDV), the global state routing scheme (GSR), the fisheye state routing (FSR) and hierarchical state routing (HSR). Hong et al. have given an excellent overview of scalable MANET routing protocols in [5].

Transport layer protocols can be used to provide reliable transmission and session control to network applications. In the case of sensor networks, many applications will be served well by a datagram connectionless unreliable transport, and reliable mechanisms may be required only for certain specific traffic such as audio and video monitoring, with additional implications in terms of resource reservation and quality of service.

1.2.3 Layers 5 through 7: session, presentation and application

Security applications require that sensor coverage be assured at all times at least by a subset of the sensor nodes. The specific limitations associated to sensor networks have to be tackled, while aiming at high detection probabilities and low false alarm rates. Data reduction techniques such as thresholding can provide high detection probabilities as well as high false alarm rates. Collaboration techniques enable data fusion between sensors and improved target location and tracking.

As a general rule, it is normally more efficient to process data on the local sensor rather then transmitting them to a central processing centre. Pottie and Kaiser give an example in [6], where they estimate that the energy cost of transmitting 1 Kb at the distance of 100 metres using a 1 GHz carrier frequency and a $\lambda/2$ antenna, with BPSK under Raleigh fading and noiseless receiver, is the same to execute 3 million operations using a general purpose processor with 100 MIPS/W power.

Local processing enables data reduction, and multi-hop routing and advanced coding techniques, reduce energy costs. The decision on the amount and types of data to be transmitted is principally driven by the battery and energy constraints resulting from the design of the sensor node.

As an example we can take a generic linear array used for passive sonar surveillance, as those found in COTS security systems for diver detection around oilrigs and commercial ports. The raw data rate acquired by a 64-hydrophone linear array can be estimated as 3 Mbit/s (24 bits * 64 hydrophones * 2000 Hz). The choices are between transmitting the whole stream of data to the neighbouring nodes to enable signal correlation and applying on-sensor data reduction (e.g. signal decimation) to achieve compression rates of two orders of magnitude, that is reducing the bandwidth requirement from 3 Mbit/s to 30 Kbit/s. It appears evident how the onboard processing capability greatly reduces the requirements in terms of communications between nodes, offering also an effective approach towards the utilization of the sensor energy and improved communications reliability.

1.3 Antenna issues

Antenna design and positioning are two crucial and often underestimated factors influencing the actual communications capabilities of sensor nodes. The antenna has to be small, efficient and capable of supporting the relatively low RF frequencies to be used. Using a poorly engineered antenna reduces the RF communications range of the wireless node: this reduction would have then to be compensated by a more sensitive receiver or by increasing transmit power, which could both result in higher power consumption.

Omnidirectional antennas offer the maximum flexibility in the deployment of the nodes, which can and should occur on the basis of considerations, which are mostly specific to the type of surveillance that has to be performed. On the other hand, as discussed by Kumar and Gupta in [7], the maximum throughput obtainable by a node is the function of network data rate and size, regardless of the channel access mechanism or routing protocol in use, as a consequence of the interference of concurrent transmissions from neighbouring nodes.

Miller has analysed [7] the probability of establishing a 2-hop connection in a randomly distributed (Gaussian) deployment of mobile radio terminals. The concept can be adapted to sensor networks with a different distribution, or to networks where the node positioning is deterministic, noting however that communication is assumed either in plaintext or with encryption by a single *mission key* shared by all the nodes.

Antenna directivity can provide significant improvements in terms of frequency re-use, multipath mitigation and better signal to noise to ratio, which translate into throughput increase and end-to-end latency reduction. Compact beamforming antennas, incorporating beam steering or beam switching techniques, could be applied in a very profitable manner to sensor networks. Ramanathan and Yi et al. discuss the advantages of employing directive antennas in very large sensor networks in [9] and [10], respectively.

1.4 Deployment topologies and sensor performance

Engineers working on sensor networks have to face an enormous number of trade-offs between conflicting aspects, which strongly influence system design. Regardless of the limitations implied by the operational context for the sensor network, system effectiveness in achieving the desired probability of detection has to remain the cardinal requirement.

The optimal deployment strategies in military sensor networks are a function of the application and of the environment, to be developed using operations research analyses that are beyond the scope of this paper.

Some references to academic research in this area are provided in the Additional Reading section, references {[22],[30]}.

2.0 SENSOR SECURITY ISSUES

Unattended sensors may be deployed in hostile areas, exposing them to monitoring, capture and covert manipulation by the opponents. Sensor compromise can result in node obliteration or denial of service, or worse, in the intrusion of the attacker in the sensor network, using the authenticated node as a starting platform to inject false data to his advantage. The issues of communications security (COMSEC) and information security (INFOSEC) have to be addressed from the early design stages, since the physical exposure of the nodes to unfriendly forces makes traditional infrastructure-based approaches to security inapplicable.

The areas to be covered relate to secure routing, node cooperation and key management. Some existing protocols are not sufficiently flexible to handle the node additions and cancellations in the battlespace network. On the other hand, traditional authentication models based on credentials are not applicable to provide the required identity management and information assurance.

2.1 Analysis of the threat

Threat analysis and the resulting approaches towards security are more complex than in the case of standard networks, in consideration of additional risk factors such as physical displacement of sensors.

Physical displacement is one of the basic attacks against sensor networks: an attacker could move sensors from their original position, or destroy them, and replace them with rogue nodes which could be used as bridgeheads to feed false data or to compromise the functionality of the whole network. This type of attack is not only relevant to military sensor networks, but also to homeland security surveillance networks deployed in public locations such as airports, hospitals or harbours.

In some cases, physical proximity (with no physical access) to the actual sensor is sufficient. An attacker could, as an example, modify the environment *around* the sensor, forcing it to report false information, or could bring it to transmit continuously, to come to a state of denial of service following battery exhaustion.

Positional information has to be protected both in confidentiality as well as in integrity: on one side, the positioning of the sensor has to be protected to preserve the tactical advantage given by the covertness of the nodes, on the other, assurance has to be given that information fed into a recognized operational or environmental picture is not poisoned by false or inaccurate positional data.

The basic principle stated by Pfleeger et al [11] still holds: information has to be protected to a degree consistent with its value. Different protection techniques can therefore be adapted to safeguard each possible type of data stored or transmitted by the sensor nodes, optimising energy resources.

Slijepcevic et al. [12] have developed this design, by classifying the various data types and identifying specific security threats from each classification. In their model each data type is protected by a corresponding security mechanism: since each method has different resource requirements, efficient resource management is made possible, which is essential for wireless sensor networks.

The level of protection for different data types is truly a function of the application to be supported, and the protection profile for the same sensor system can radically change as a function of the deployment type.

Just to make an example: an underwater surveillance system composed of several buoys could be deployed to protect an area (e.g. a port) or to detect a specific target type (e.g. a submarine, scuba divers). The process would be conducted through the steps of event detection, event or target classification (following interaction with the neighbouring nodes), and event reporting. In this case the security focus would be principally on the integrity of the transmitted event information, and on the time required to report to a control centre (the fresher and the more accurate the information, the better).

On the other hand, the same system could be deployed in a test range for calibration purposes, using friendly forces as a target. In this case the focus would be more on the protection of the information actually stored and processed on every sensor buoy, rather than on the information transmitted. Should a buoy be lost or captured, the sensitive information collected on friendly forces (such as target characterization) has to be protected in a way that makes the recovery by an unauthorized party very unlikely, or better, impossible.

2.2 Encryption for sensor networks

Link layer encryption is crucial provide confidentiality and integrity during the transmission of both sensor data and routing information. Encryption provides an effective protection also against the Sybil attacks in which a node impersonates another node or claims a false identity, as discussed by Newsome et al. in [13].

Key exchange and distribution protocols such as Diffie-Hellman or public-key encryption in general are not readily applicable to sensors networks, because of the unpredictable topology, communications range limitations, and discontinuous operations (e.g. to account for sensor sleep periods to save energy or to reduce the probability of detection). In addition to that, public key encryption is computationally expensive and not well suited to resource-constrained nodes (e.g. the memory in miniature nodes is usually insufficient to store the long keys required by secure asymmetric encryption).

Perrig et al. [14] have proposed SPINS, a symmetric protocol specifically addressed to resource-limited sensor networks. The concept includes a base station that shares a secret key with every sensor node: to

establish a new key, two nodes use the base station as a trusted agent to set up the new key. But the requirement for more powerful base stations may be a limiting factor for many applications, where, for example, the topology is not known in advance.

Key pre-distribution is one possible alternative, but it is not well scalable. A single secret key (*mission key*) for the whole network makes selective key revocation impossible, and the compromise of a single node would result in the compromise of the whole network. Pre-loading of pair keys to be used in point-to-point links could in option: every node in a *n*-size network would be pre-loaded with *n-1* pair keys, and each *n-1* key would be secretly shared with just another node, enabling selective key revocation. But also this approach has its shortcomings: first, it is not scalable to very large networks, in consideration of the large number of pair keys that would have to be generated and loaded on every node. Second, pair-wise keys would work only on a fully connected network with direct node-to-node communication: data exchange could only occur within a small range and multi-hop communication capabilities would not be properly supported.

Eschenauer and Gligor have proposed an interesting key management schema [15], which can scale to very large distributed networks, satisfying both the operational and the security requirements for sensor networks. Only a randomly selected subset of all possible *n-1* key pairs is loaded on sensor nodes: in the initial shared-key discovery phase every node discovers its neighbours in wireless communication range with which it shares keys: this is done by broadcasting in clear text a list of short identifiers (key list numbers) for the keys actually loaded on the node. Once the receiving node finds in his local storage a key supported by the remote, the link is established using a challenge-response technique.

Upon establishment of the secure point-to-point link a subsequent *path-key establishment phase* is conducted where a *path-key* is established and assigned to selected pairs of sensor nodes in wireless communication range that do not share a key but are connected by two or more links at the end of the shared-key discovery phase. The clear text initialisation could however pose problems with regard to denial of service attacks. Eschenauer and Gligor also describe a key revocation mechanism, based on a central controller node, which has a large communications range and may be mobile. Revocation is performed by a single revocation message containing a signed list of *k* key identifiers for the keys to be revoked. The latency of this approach is a function of the effectiveness of the communication between the central controller and the other nodes of the sensor network. Once the keys are revoked, some links may disappear and the affected nodes need to re-enter in the shared-key discovery phase and possibly path-key establishment phase. This *(n-1)*-pairwise scheme is perfectly resilient against node capture.

Chan, Perrig and Song, have developed in [16] a random key pre-distribution mechanism that is built on the Eschenauer-Gligor method, to support node-to node authentication. Together with every key *k* stored on a node a number (*node ID*) is associated, to note the identification number of the other node that stores *k*. In the initial shared-key discovery phase the node ID list is transmitted, instead of the key short identifiers list. By searching for the received IDs in their key table, all nodes within communications range can tell whether they share a common pairwise key for communication. A cryptographic exchange is then used to actually verify the actual knowledge of the key. The effective communications range can be extended beyond the physical communications range by having neighbouring nodes rebroadcast the received node IDs for a certain number of hops, so that *path keys* can be negotiated. Each hop effectively extends the range by one communications radius, increasing the number of nodes that can hear the broadcast by a squared factor. The establishment of path keys for multi-hop range extension should however be used with caution, because the rebroadcast is performed with no verification of the authentication information.

With regard to key revocation, the Chan-Perrig-Song method is based on a distributed scheme, where the nodes have a mechanism in place to detect whether another node has been compromised. A public voting is performed and if any node *B* observes a number of votes against node *A* exceeding a certain threshold *t*, then *B* breaks communications with *A*. The design of such a decision system is however very challenging.

Du et al. have also developed [17] a key pre-distribution scheme that provides a threshold property where if the number of compromised nodes is lower than the threshold λ, the remaining uncompromised nodes are perfectly secure. This mechanism however lacks the perfect resiliency against node capture.

All those proposed mechanisms do not provide the certainty that two nodes can generate a pairwise key, but instead a probability *p* is given that *n* nodes are connected. This probability can be modelled using random graph theory. The mainstream of this research field follows the work by Erdös and Rényi [18] to relate the relationship between local connectivity (i.e. the probability of two nodes being connected) and global connectivity (i.e. the probability that the whole network is connected).

2.3 Tamper protection

Sensor nodes are exposed to all kinds of physical security threats and tamper detection techniques play an important role to support the security of the network and of the information being exchanged. Once an adversary obtains physical control, attempts could be made to alter the hardware and software configuration, or to extract sensitive information from the memory of the sensor.

A mix of active and passive techniques is required. Active technologies are based on a resident electronic *watchdog*, to detect the attempted tampering and to perform the actions such as memory zeroizing. Some low cost microcontrollers such as the Fortezza Card integrate support primitives for cryptography and attempt to zeroize their memory it tampering is detected, in accordance with the FIPS 140-2 Level 4 standard [19].

Intentional excursions beyond the normal operating ranges may be used by an attacker to stop the defences of the cryptographic module: protection needs to be foreseen against a security compromise due to environmental conditions or fluctuations outside of the module's normal operating ranges for voltage and temperature.

Vulnerabilities exist also to battery exhaustion attacks: forcing the sensor to consume excessive energy, (e.g. by causing excessive transmissions) can be initially characterized as a denial or service attack, which then opens the path to a complete sensor compromise in case the antitampering mechanism is impaired by the lack of energy.

Passive techniques prevent or delay physical access to the system hardware and include a mix of secure coating and secure design as in the Raytheon SecureIT chip [20].

3.0 CONCLUSIONS

Extensive research is available and is still being conducted on the topics of mobile ad-hoc networks and of sensor networks. Sensor networks can be characterized as a special class of ad-hoc networks in which the nodes integrate actuators, sensors, data processors and communications capabilities. The additional complexity in comparison with many MANETs derives from the conditions of unattended operations is areas that are environmentally or tactically hostile, and from the additional scalability and resiliency requirements.

In this paper we have tried to summarize the various aspects that need to be considered in the design of sensor networks that have to operate in autonomy and with no human support, to provide security services in the fields of Network Enabled Capabilities and Network Enables Warfare. For sure the “one-size-fits-all” principle does not apply, because the engineering constraints to be faced are very specific to the applications to be provided and have therefore to be tackled explicitly.

As an example, the concepts being developed for the NATO Network Enabled Capabilities are centred on the Internet protocols, which are normally conceived for low-latency, well-connected environments, where power consumption is not the first concern. On the other hand, the capacity of the batteries is the greatest limiting factor to the sensor life expectancy, and power-awareness has to be included at all the layers of the communications stack.

At the lowest layers, control of the transmit power levels is a definite requirement, to adjust the RF emission to the desired communications range. The recent developments in MAC protocols may offer viable ways to use available energy sparingly.

Power-aware routing is also a requirement, to handle situations where the need for frequent path updates conflicts with the low duty cycle policies required to extend battery life. The introduction of spatial (location-aware) addressing could be one of the enabling factors towards simplified network management and routing.

As an example, transmit power could be optimised on the basis of the actual distance between the nodes. Location-aware addressing could also be used to simplify the re-organization of the network, e.g. by supporting primitives such as “locate all sensors within a 1 n.mi. radius”. Positional addressing would also simplify the detection of the displacement or removal of a node.

As noted by Čapkun and Hubaux in [21] it is also possible to develop GPS-free positioning systems where each node computes positions of its neighbours in its local coordinate system. As a practical example, Ultra wideband (UWB) technology has been shown to possess advantages for precision localization applications, where the use of short pulse RF waveforms provides inherent precision for time difference of arrival measurements.

On board processing will play a crucial role in mitigating the communications requirements of the sensor, and additional research is required to optimise and transfer the algorithms for distributed detection, decision and target tracking to the power-limited unattended sensors.

As a supplement to the engineering considerations, when discussing the application of sensor networks in a military context, information and communications security issues hold paramount importance. Traditional infrastructure-based approaches to security are not directly applicable and crypto key management schemes (and anti-tampering protection measures) need to be developed to ensure protection against the physical compromise threats to which the nodes are exposed.

REFERENCES

[1] A.B. Carlson, “Communication Systems”, McGraw-Hill International, 1986

[2] W. Ye, J. Heidemann, D. Estrin, “An Energy-efficient MAC Protocol for Wireless Sensor Networks”, Proceedings of the Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2002), June 2002, New York, NY, USA.

[3] T. van Dam, K. Langendoen, “An Adaptive Energy-Efficient MAC Protocol for Wireless Sensor Networks”, Proceedings of the 1st ACM Conference on Embedded Networked Sensor Systems, SenSys’03, November 5-7, 2003, Los Angeles, CA, USA

[4] V. Rajendran, K. Obraczka, J.J. Garcia-Luna-Aceves, "Energy-Efficient, Collision-Free Medium Access Control for Wireless Sensor Networks", Proceedings of the 1st ACM Conference on Embedded Networked Sensor Systems, SenSys’03, November 5-7, 2003, Los Angeles, CA, USA

[5] X. Hong, K. Xu, M. Gerla, “Scalable Routing Protocols for Mobile Ad Hoc Networks”, IEEE Network, July/August 2002

[6] G.J. Pottie, WJ Kaiser, “Wireless Integrated Network Sensors”, Communications of the ACM, May 2000, Vol 43, No. 5

[7] P. Gupta, P.R. Kumar, “The Capacity of Wireless Networks", IEEE Transactions on Information Theory, vol. IT-46, no. 2, pp. 388-404, March 2000.

[8] L.E. Miller, "Probability of a Two-Hop Connection in a Random Mobile Network," 35th Conf. on Info. Sci. and Syst. (CISS '01), Baltimore, 21-23 March 2001

[9] R. Ramanathan, “On the Performance of Ad Hoc Networks with Beamforming Antennas”, Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing,, October 4-5, 2001, Long Beach, CA, USA

[10] S. Yi, Y. Pei, S. Kalyanaraman, “On the Capacity Improvement of Ad Hoc Wireless Networks Using Directional Antennas”, Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing, June 1-3, 2003, Annapolis, MD, USA

[11] C.P. Pfleeger, S.Lawrence Pfleeger, “Security in Computing”, Prentice Hall PTR, 2002

[12] S. Slijepcevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck, M.B. Srivastava “On Communication Security inWireless Ad-Hoc Sensor Networks”, Proc. of the Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE’02), June 10 - 12, 2002, Pittsburgh, PA, USA

[13] J. Newsome, E. Shi, D. Song, A. Perrig, “The Sybil Attack in Sensor Networks: Analysis & Defenses”, Proceedings of the third international symposium on Information processing in sensor networks IPSN’04, April 26 - 27, 2004, Berkeley, California, USA

[14] A. Perrig, R. Szewczyk, J.D. Tygar, V. Wen, D.E. Culler, “SPINS: Security Protocols for Sensor Networks”, Wireless Networks 8, 521–534, Kluwer Academic Publishers, 2002

[15] L. Eschenauer, V. D. Gligor, “A Key-Management Scheme for Distributed Sensor Networks”, ACM Conference on Computer and Communications Security CCS’02, November 18-22, 2002, Washington, DC, USA

[16] H. Chan, A. Perrig, D. Song, “Random Key Predistribution Schemes for Sensor Networks”, Proceedings of the 2003 IEEE Symposium on Security and Privacy, May 11 - 14, 2003, IEEE Computer Society, Washington, DC, USA, ISBN 0-7695-1940-7

[17] W. Du, J. Deng, YS. Hang, PK Varshney, “A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks”, ACM Conference on Computer and Communications Security CCS’03, October 27-31, 2003, Washington, DC, USA

[18] P. Erdös, A. Rényi, “On the evolution of random graph”, Institute of Mathematics, Hungarian academy of Sciences, 1959

[19] National Institute of Standards and Technology (NIST), “Security Requirements for Cryptographic Modules”, Federal Information Processing Standards Publication 140-2 (FIPS PUB 140-2), May 2001, http://csrc.nist.gov/cryptval/

[20] http://www.raytheon.com/products/secure_it/

[21] S. Čapkun, J.P. Hubaux, "Secure Positioning in Sensor Networks", Laboratory for Computer Communications and Applications (LCA), Swiss Federal Institute of Technology Lausanne (EPFL), CH-1015 Lausanne, Switzerland

Additional Reading

[22] T. Clouqueur, V. Phipatanasuphorn, P. Ramanathan, K.K. Saluja "Sensor Deployment Strategy for Target Detection", Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications, September 28 - 28, 2002, Atlanta, Georgia, USA

[23] K. Chakrabarty, S. S. Iyengar, H. Qi and E. Cho, "Grid coverage for surveillance and target location in distributed sensor networks", IEEE Transactions on Computers, vol. 51, pp. 1448-1453, December 2002.

[24] S. Meguerdichian, F. Koushanfar, M. Potkonjak and M. B. Srivastava, "Coverage problems in wireless ad-hoc sensor networks", Proc. IEEE Infocom Conference, vol 3, pp. 1380-1387, 2001.

[25] S. Meguerdichian, F. Koushanfar, G. Qu and M. Potkonjak, "Exposure in wireless ad-hoc sensor networks", Proc. IEEE Mobicom Conference, pp. 139- 150, July 2001.

[26] Y. Zou, K. Chakrabarty, "Uncertainty-aware and coverage-oriented deployment for sensor networks", Journal of Parallel and Distributed Computing, Academic Press, Volume 64, Issue 7, July 2004

[27] S.S. Dhillon, K. Chakrabarty, "Sensor placement for effective coverage and surveillance in distributed sensor networks", Proceedings of the IEEE Wireless Communications and Networking Conference, WCNC 2003, 16-20 March 2003

[28] T. Yan, T. He, J.A. Stankovic, "Differentiated Surveillance for Sensor Networks", Proceedings of the 1st ACM Conference on Embedded Networked Sensor Systems, November 5-7, 2003, Los Angeles, CA, USA

[29] X. Wang, G. Xing, Y. Zhang, C. Lu, R. Pless, C.D. Gill, "Integrated coverage and connectivity configuration in wireless sensor networks", Proceedings of the 1st ACM Conference on Embedded Networked Sensor Systems, SenSys'03, November 5-7, 2003, Los Angeles, CA, USA

[30] C. Gui, P. Mohapatra, "Power conservation and quality of surveillance in target tracking sensor networks", Proceedings of the 10th ACM Conference on Mobile computing and networking, MOBICOM'04, September 26 - October 01, 2004, Philadelphia, PA, USA

The challenges of internetworking unattended autonomous sensors

Alessandro Berni, Diego Merani, Michel Leonard
NATO Undersea Research Centre

Requirement

- "NNEC encompasses the elements involved in linking collectors, effectors and decision makers together, to enable the development of a NATO, network-centric, effects-based, operational capability."

Contre-Amiral Xavier Païtard
Future Capabilities, Research & Technology
HQ SACT

- Solutions have to consider several trade-offs between the various components of resource-limited sensors

Proposed approach

- An holistic approach is proposed, to realize a balanced compromise between sensor capabilities and their integration with network infrastructures.

- Design process aligned to the ISO/OSI protocol stack, with consideration to security (both INFOSEC and COMSEC) starting from the early phases of the design.

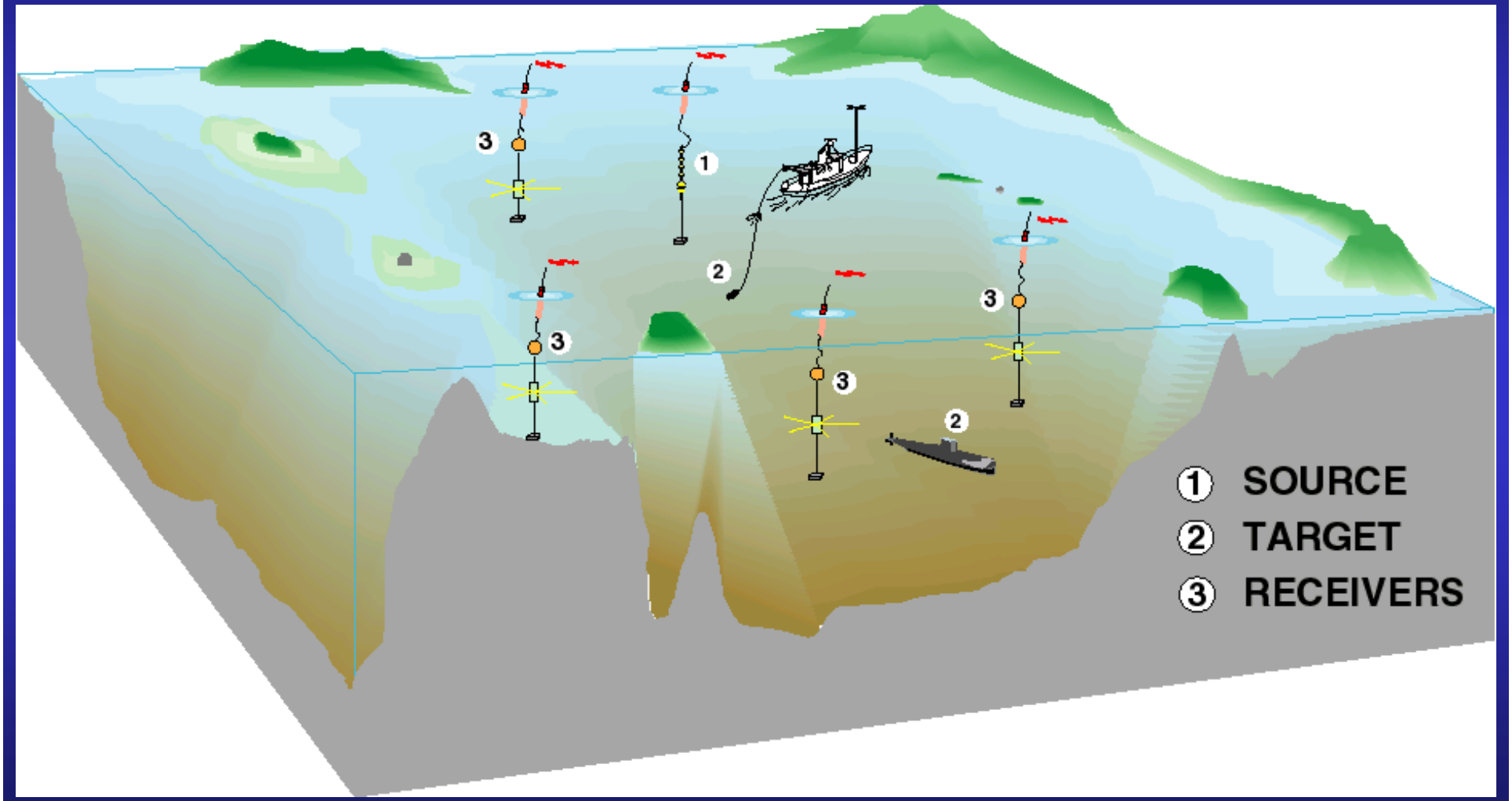
Scope and purpose

- The primary purpose of sensor networks is to detect and report events occurring within detection range
  - basic functions include event detection and reporting, target classification and tracking.
  - they offer a cost-effective approach to detect low-signature targets (reducing errors and improving tracking and targeting) and to support the Operational Picture.

Mission types

- Basic mission types involve:
  - the defence of a perimeter or the denial of an area (e.g. for port protection), and
  - covert remote surveillance (e.g. in preparation of amphibious operations).
- The behaviour of nodes can vary on the basis of the mission assigned:
  - upon the detection of an event of interest, the sensor may relay the information directly to the Command or may start collaborating with other nodes to reduce its probability of false detection, or to perform target tracking.

Maritime Surveillance Network



Constraints to be faced

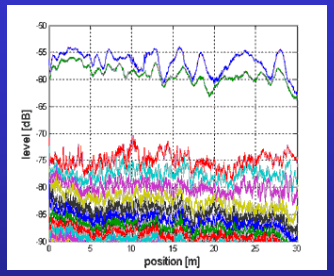
- Operation of sensor networks normally occurs in a physically demanding environment
  - sensors are exposed to detection and compromise: risks of denial of service, node displacement or removal, false data injection,
  - difficult communications environment
- The greatest limiting factor to the sensor's capability and life expectancy lies in the capacity of the batteries.

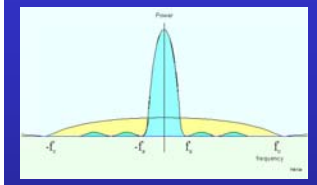
Communications architecture

- Sensor networks have many points in common with ad-hoc networks
- Complementary requirements to ensure additional flexibility
  - Example: the membership and role of a sensor in a network may not be known before the network is actually deployed.
- Can be modeled on the basis of the ISO/OSI protocol stack

Layers 1-2

- In Sensor Networks, communications usually occur using wireless medium
- The use of spread spectrum can be used to optimize battery life
- Spread spectrum, wideband technologies also reduce probability of detection
- Adherence to standards + choices in frequency bands = license-free installation anywhere in the world
- FMSC of the NATO C3 Board is addressing the implications of the introduction of new wideband digital communications systems





ISM-900

Freq. range:	902-928 Mhz
Bandwidth:	26 MHz
Max Power:	1 Watt
Max EIRP	4 Watt (+36 dBm)

ISM-2.4

Freq. range:	2400-2483.5 MHz
Bandwidth:	83.5 MHz
Max Power:	1 Watt
Max EIRP	4 Watt (+36 dBm) for multi-point 200 W (+53 dBm) for point-to-point

ISM-5.8

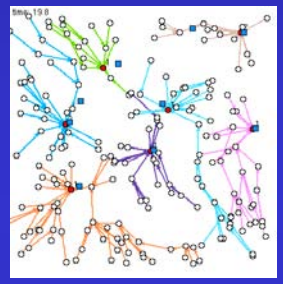
Freq. range:	5.725GHz-5.850 GHz
Bandwidth:	125 MHz
Max Power:	1 Watt (+30 dBm)
Max EIRP	200 W (+53 dBm)

The ISM band of 2.4 does not guarantee protection from interference

Very powerful low-cost jammers: microwave ovens!

Layers 3-4

- Automatic network self-organization is an important requirement



Loss of a fraction of the nodes leads to graceful decrease of network performances

- Limited energy resources have to be always accounted
  - Periodic re-routing balances energy consumption across the network

Spatial addressing

- IP addressing is purely logical (A.B.C.D)
- Spatial (location aware) addressing could bring simplified network management and routing
- GPS availability is not an absolute pre-requisite
  - Proof of concept already given using UWB technology

Layers 5-7

- Objective of the sensor application:
  - High detection probabilities
  - Low false alarm rates
- On-board processing is normally more efficient than transmitting raw data to a central processing centre (studies by Pottie and Keiser)
  - Reduction of communications requirements results in better utilization of energy and improved communications reliability

Example of onboard processing gain

- Generic linear sonar array
  - 64 hydrophones, 24 bit sampling, 2000 Hz
  - Raw date rate is approx. 3 Mbit/s
  - On-board processing enables data reduction (e.g. by signal decimation)
  - 3 Mbit/s $\Rightarrow$ 30 Kbit/s

Sensor security issues

- Threat analysis and the resulting approaches towards security are more complex than in the case of standard networks
  - additional risk factors, such as physical displacement of sensors.
  - level of protection for different data types is a function of the application to be supported
  - the protection profile for the same sensor system can radically change as a function of the deployment type.

Protection profiles

- Classification of data types and corresponding threats leads to the identification of more specific security mechanisms (see work by Slijepcevic et al.)
- Since each mechanism has different resource requirements, efficient resource management is made possible

Encryption for sensor networks

- Link layer encryption is crucial during the transmission of both sensor data and routing information
- Traditional key exchange and distribution protocols are not readily applicable
- Specific protocols for sensor networks have been proposed (e.g. SPINS)

Key pre-distribution

- Pre-distribution of a single *mission key* is a possibility
  - does not scale well
  - makes selective key revocation impossible
- Pre-loading of pair keys is an alternative
  - Also subject to scalability problems
  - Would work only on a fully connected network
- Interesting work from Eschenauer and Gligor
  - Refined by Chan, Perrig and Song

Eschenauer-Gligor method

- Only a subset of the n-1 key pairs is loaded on the sensor nodes
- Phase 1: shared-key discovery
  - Transmitting in clear text a list of short key identifiers
- Phase 2: path-key establishment
  - Enables multi-hop communication
- Selective key revocation is possible
  - Using a central controller node
- This method is fully resilient against node capture

Chan-Perrig-Song method

- Builds on Eschenauer-Gligor to support node-to-node authentication
- A Node ID is associated to each key pair
  - The Node ID is used in the shared-key discovery, rather than the key identifier
- Effective communications range can be extended (multi-hop range extension)
- Distributed key revocation mechanism, based on voting system

Anti-tamper protection

- Due to the physical exposure of the sensors, anti-tamper protection plays an important role
- Mix of passive and active techniques required
  - FIPS 140-2 Level 4 Standard
  - Raytheon SecureIT chip

Conclusions

- Extensive research is available and is still being conducted on this topic
- The “one-size-fits-all” principle does not apply
- Power-awareness is mandatory
- On-board processing crucial to mitigate communications requirements
- Traditional infrastructure-based approaches to security are not applicable and crypto key management schemes (and anti-tamper protections) need to be developed.